Tips on Creating a Strong Password For Your eAuthentication Account

Overview

To help protect your eAuthentication account, we have created the following rules that enforce password security. They are:

- 12 to 24 characters long
- Contain at least one uppercase letter
- Contain at least one lowercase letter
- Contain one non-alphabetical character, which includes numbers and/or these special characters:
  ! # $ % = + : ; , ? ~ * -

- Your password may not contain your first name, last name, User ID, Mother's Maiden Name, Date of Birth, 4-digit PIN, security questions or answers.
- Do not use dictionary words, spaces, or tabs, or any other special characters not listed above.
- Your password will expire after 180 days.

The key to making your eAuthentication account as secure as possible is creating the strongest possible password while making it easy to remember. The following are guidelines that will help you do this:

Password tips

- **Make your password lengthy**. Your password must be a minimum of 12 characters; however the longer you make the password, the harder it will be for someone to guess. Therefore, try to make your password up to 12 characters long.

- **Avoid repeated characters or common character sequences**. Do not use more than one or two letters or numbers together (for example: “11111111” or “aaaaaaa”.) Also avoid common sequences such as “qwertyuiop” , “123456789”, or “abcdefghij”. These sequences are too easily guessed.

- **Avoid use of dictionary words of any language.** Many hackers use dictionary words of many mainstream languages, including slang, to guess passwords. If you use these in your password, it makes it easier to guess by a hacker.

- **Make your password difficult to guess or research**. One technique is to pick a favorite quote, song lyric, or phrase and use the first character from each word or syllable to build a password. See our sample passwords section. This will help you select a nonsense word that can’t be compared to any known dictionary word and should be un-related to any identity details known or researchable about you.

- **Avoid obvious character substitutions.** Replacing the letter “i” with 1 or the letter “o” with 0 does little to prevent a password guessing attack.

- **Do not use the same password in all systems.** If one of the online systems or computers you use is compromised, then the attacker could potentially have access to all of your systems. Make sure you use a distinctly different password for all of your systems.

Sample Passwords

Example:

1. If you select the phrase: “the quick brown dog jumped over the lazy dogs back”, then you could build a password from the first letter of each word, “tqbfjotldb”
2. Add at least 1 number and special character, “tqbfjotldb*7”
3. Change some of the letters to upper case, “TqBfjOtlDb*7”
4. This will result in a strong password.

Do’s and Don’ts

Do’s	Don’ts
• **DO** pick a password you will remember • **DO** change your password on a regular basis • **DO** use a mix of uppercase and lowercase characters. • **DO** use different passwords for different systems and accounts. • **DO** use special characters such as, ! # $ % = + : ; , ? ~ * • **DO** select words from a phrase, song, or poem and use the first letter of each word, to create an strong password. (e.g., "Oh say can you see by the dawns early light?" becomes the password oScyCbtDeL9+). • **DO** use a password that you can type quickly without having to look at your keyboard. This makes it harder for someone to notice your password if they happen to be watching over your shoulder. • **DO** use a password with 8 or more characters. More is better.	• **DON'T** write your password down. • **DON'T** use your first name, last name, User ID, Mother's Maiden Name, Date of Birth, 4-digit PIN, security questions or answers in your password • **DON'T** share your password with anyone. • **DON'T** use a word contained in English or foreign language dictionaries, spelling lists or commonly digitized texts such as the Bible or an encyclopedia. • **DON'T** use a word spelled backwards. • **DON'T** use an alphabet sequence (cdefghijk), a number sequence (987654321) or a keyboard sequence (zxcvbnm). • **DON'T** use a password shorter than six (9) characters. • **DON’T** Re-use any of your last 5 passwords. • **DON'T** use a password of all the same digits, the same letter. • **DON'T** use the same password for more than one system or web site. • **DON’T** Use numbers in place of letters. For example, “Password” becomes “Pa55w0rd.” • **DON’T** Use dates to create a password (for example, AUguST2001). • **DON’T** Use sample passwords given on various Web sites, including this one.

Other References

To find out more information about creating stronger passwords and protecting your identity, type the following search terms into your favorite internet search engine.

- “Creating a strong password”
- “Password Security”
- “Protecting personally identifiable information”